

311912

# LOCKING DEVICE FOR VENDING MACHINE

Publication number: JP10110563 (A)

IDS 未

Publication date: 1998-04-28

Inventor(s): SASAKI KAZUO; HIRANO MASAMI +

Applicant(s): UNITEC KK; TAKIGEN MFG CO +

Classification:

- international: E05B49/00; E05B65/02; G01S13/75; G01S13/76; G01S13/79; G07F9/00;  
E05B49/00; E05B65/02; G01S13/00; G07F9/00; (IPC1-7): E05B49/00; E05B65/02;  
G01S13/75; G01S13/76; G01S13/79

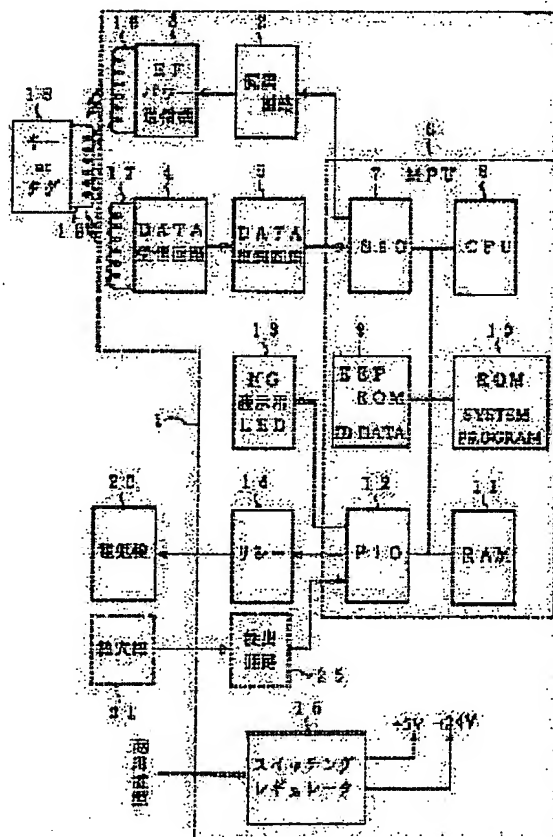
- European:

Application number: JP19960284648 19961007

Priority number(s): JP19960284648 19961007

## Abstract of JP 10110563 (A)

**PROBLEM TO BE SOLVED:** To prevent the breakage of a lock, and to minimize the damage even when a lock hole is broken. **SOLUTION:** A vending machine is provided with a dummy key hole. When a key is inserted in the key hole, a reader 1 of the vending machine transmits the RF power signal. A transponder 18 of the key is operated by receiving the RF power signal, and the ID data (the system discrimination ID data, the master key group ID data, and the key ID data) stored in an EEPROM are transmitted according to the data requesting command from the reader 1. The reader 1 receives the ID data, and compares the received data with the ID data preset in an EEPROM 9, and when all the data agree, a relay 14 is driven to open an electric lock 20. Because the key hole is simply a dummy to detect the unlocking, the damage can be minimized even when the lock is broken.



Data supplied from the *espacenet* database — Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-110563

(43)公開日 平成10年(1998) 4月28日

(51)Int.Cl.<sup>6</sup> 識別記号

E 0 5 B 49/00  
65/02  
G 0 1 S 13/75  
13/76  
13/79

F I

E 0 5 B 49/00 J  
65/02 C  
G 0 1 S 13/80

審査請求 未請求 請求項の数9 F D (全 15 頁)

(21)出願番号 特願平8-284648

(22)出願日 平成8年(1996)10月7日

(71)出願人 391030538

ユニテック株式会社  
東京都大田区中央2丁目25番6号

(71)出願人 000108708

タキゲン製造株式会社  
東京都品川区西五反田1丁目24番4号

(72)発明者 佐々木 和夫

東京都大田区中央2丁目25番6号 ユニテ  
ック株式会社内

(72)発明者 平野 正己

東京都大田区中央2丁目25番6号 ユニテ  
ック株式会社内

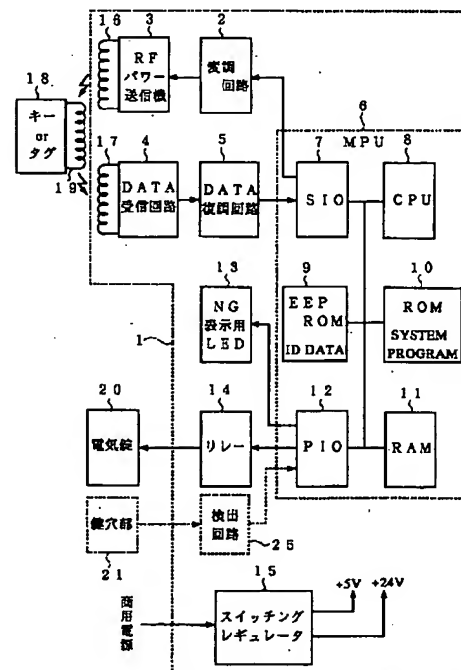
(74)代理人 弁理士 鹿嶋 英實

(54)【発明の名称】 自動販売機の鍵装置

(57)【要約】

【課題】 錠の破壊を防止することができ、また、仮に錠穴が破壊されても、被害規模を最小にすることができる自動販売機の鍵装置を提供する。

【解決手段】 上記自動販売機には、ダミーの錠穴が設けられている。自動販売機のリーダ1は、錠穴に錠が挿入されると、RFパワー信号を送信する。錠のトランスポンダ18は、上記RFパワー信号を受信することで作動し、EEPROM24に記憶されているIDデータ(システム識別IDデータ、マスタ・キー・グループIDデータおよび錠IDデータ)を、リーダ1からのデータ要求コマンドに応じて送信する。リーダ1は、上記IDデータを受信し、EEPROM9に予め設定されているIDデータと比較し、全てが一致すると、リレー14を駆動して電気錠20を開く。上記錠穴は、単に、開錠されることを検知するためのダミーであるので、仮に破壊されたとしても、最小の被害で済む。



## 【特許請求の範囲】

【請求項1】 外部の高周波磁界を各部を駆動するための電力とする装置であって、当該装置を識別するための応答装置識別データを記憶する第1の記憶手段および電力が印加されると前記第1の記憶手段に記憶されている応答装置識別データを送信する第1の送信手段を備える応答装置と、

前記高周波磁界を発生する高周波発生手段、前記第1の送信手段から送信された応答装置識別データを受信する第1の受信手段、自動販売機の扉を施錠する電気錠、前記自動販売機の扉を開けることを許可する応答装置を特定する応答装置識別データを記憶する第2の記憶手段、前記第1の受信手段によって受信された応答装置識別データと前記第2の記憶手段に記憶されている応答装置識別データとが一致した場合、前記電気錠を開ける第1の制御手段を備え、前記自動販売機に設けられる読み取り装置とを具備することを特徴とする自動販売機の鍵装置。

【請求項2】 前記読み取り装置は、前記第1受信手段によって受信された応答装置識別データと前記第2の記憶手段に記憶されている応答装置識別データとが一致しない場合、警告を発する警告手段を具備することを特徴とする請求項1記載の自動販売機の鍵装置。

【請求項3】 前記応答装置は、鍵形状部分を有し、前記自動販売機は、前記電気錠が設けられる位置とは異なる位置に、前記応答装置の鍵形状部分が挿入される鍵穴部を備え、前記読み取り装置は、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことを検知する検出手段を備えることを特徴とする請求項1記載の自動販売機の鍵装置。

【請求項4】 前記読み取り装置は、前記検出手段によって、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことが検知されると、前記高周波発生手段によって高周波磁界を発生することを特徴とする請求項3記載の自動販売機の鍵装置。

【請求項5】 前記応答装置は、カード形状であり、前記読み取り装置は、前記高周波発生手段によって所定時間間隔で前記高周波磁界を発生することを特徴とする請求項1記載の自動販売機の鍵装置。

【請求項6】 前記応答装置および前記読み取り装置は、前記応答装置識別データに加えて、システムを識別するシステム識別データおよび自動販売機の設置地域を識別するマスタ・キー・グループ識別データを授受することを特徴とする請求項1ないし5記載の自動販売機の鍵装置。

【請求項7】 前記応答装置は、所定の通信プロトコルに従って、前記読み取り装置との間におけるデータ授受を制御する第2の制御手段を備え、前記応答装置および前記読み取り装置は、前記所定の通信プロトコルに従って、前記システム識別データ、前記

マスタ・キー・グループ識別データおよび前記応答装置識別データを授受することを特徴とする請求項1ないし5記載の自動販売機の鍵装置。

【請求項8】 前記読み取り装置は、前記応答装置に対してデータを送信する第2の送信手段と、前記制御手段によって前記電気錠が開けられると、新たな応答装置識別データを生成する応答装置識別データ生成手段と、前記第2の記憶手段に記憶されている応答装置識別データを、前記応答装置識別データ生成手段によって生成された新たな応答装置識別データで書き換える第1の更新手段とを備え、前記第2の送信手段によって前記新たな応答装置識別データを前記応答装置に対して送信し、前記応答装置は、前記読み取り装置が送信するデータを受信する第2の受信手段と、前記第1の記憶手段に記憶されている応答装置識別データを、前記第2の受信手段によって受信した前記新たな応答装置識別データで書き換える第2の更新手段とを備えることを特徴とする請求項1ないし7記載の自動販売機の鍵装置。

【請求項9】 前記応答装置識別データおよびマスタ・キー・グループ識別データは、外部設定装置により無線通信により書換可能であることを特徴とする請求項1ないし8記載の自動販売機の鍵装置。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、商品の無人販売に用いられる自動販売機に用いて好適な自動販売機の鍵装置に関する。

【0002】

【従来の技術】従来より、商品の無人販売に用いられる自動販売機においては、筐体に設けられている鍵穴に、所定の鍵を差し込んで錠を外し、自動販売機を開けることで、商品の補充・交換、あるいは代金の回収が行われている。

【0003】

【発明が解決しようとする課題】ところで、従来の自動販売機では、鍵穴が見えるため、錠の位置が容易に判別できる。このため、筐体に設けられている錠が破壊され、内部の代金や商品が盗難されるという問題があった。特に、現金盗難の被害額より、錠修理に要する額の方が大きいので、錠の破壊を防止する必要がある。

【0004】そこで本発明は、錠の破壊を防止することができ、また、仮に錠穴が破壊されても、被害規模を最小にすることができる自動販売機の鍵装置を提供することを目的とする。

【0005】

【課題を解決するための手段】上記目的達成のため、請求項1記載の発明による自動販売機の鍵装置は、外部の高周波磁界を各部を駆動するための電力とする装置であって、当該装置を識別するための応答装置識別データを記憶する第1の記憶手段および電力が印加されると前記

第1の記憶手段に記憶されている応答装置識別データを送信する第1の送信手段を備える応答装置と、前記高周波磁界を発生する高周波発生手段、前記第1の送信手段から送信された応答装置識別データを受信する第1の受信手段、自動販売機の扉を施錠する電気錠、前記自動販売機の扉を開けることを許可する応答装置を特定する応答装置識別データを記憶する第2の記憶手段、前記第1の受信手段によって受信された応答装置識別データと前記第2の記憶手段に記憶されている応答装置識別データとが一致した場合、前記電気錠を開ける第1の制御手段を備え、前記自動販売機に設けられる読み取り装置とを具備することを特徴とする。

【0006】また、好ましい態様として、前記読み取り装置は、例えば請求項2記載のように、前記第1受信手段によって受信された応答装置識別データと前記第2の記憶手段に記憶されている応答装置識別データとが一致しない場合、警告を発する警告手段を具備するようにしてもよい。

【0007】また、好ましい態様として、前記応答装置は、例えば請求項3記載のように、鍵形状部分を有し、前記自動販売機は、前記電気錠が設けられる位置とは異なる位置に、前記応答装置の鍵形状部分が挿入される鍵穴部を備え、前記読み取り装置は、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことを検知する検出手段を備えるようにしてもよい。

【0008】また、好ましい態様として、前記読み取り装置は、例えば請求項4記載のように、前記検出手段によって、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことが検知されると、前記高周波発生手段によって高周波磁界を発生するようにしてもよい。

【0009】また、好ましい態様として、前記応答装置は、例えば請求項5記載のように、カード形状であり、前記読み取り装置は、前記高周波発生手段によって所定時間間隔で前記高周波磁界を発生するようにしてもよい。

【0010】また、好ましい態様として、前記応答装置および前記読み取り装置は、例えば請求項6記載のように、前記応答装置識別データに加えて、システムを識別するシステム識別データおよび自動販売機の設置地域を識別するマスタ・キー・グループ識別データを授受するようにしてもよい。

【0011】また、好ましい態様として、前記応答装置は、例えば請求項7記載のように、所定の通信プロトコルに従って、前記読み取り装置との間におけるデータ授受を制御する第2の制御手段を備え、前記応答装置および前記読み取り装置は、前記所定の通信プロトコルに従って、前記システム識別データ、前記マスタ・キー・グループ識別データおよび前記応答装置識別データを授受するようにしてもよい。

【0012】また、好ましい態様として、前記読み取り

装置は、例えば請求項8記載のように、前記応答装置に対してデータを送信する第2の送信手段と、前記制御手段によって前記電気錠が開けられると、新たな応答装置識別データを生成する応答装置識別データ生成手段と、前記第2の記憶手段に記憶されている応答装置識別データを、前記応答装置識別データ生成手段によって生成された新たな応答装置識別データで書き換える第1の更新手段とを備え、前記第2の送信手段によって前記新たな応答装置識別データを前記応答装置に対して送信し、前記応答装置は、前記読み取り装置が送信するデータを受信する第2の受信手段と、前記第1の記憶手段に記憶されている応答装置識別データを、前記第2の受信手段によって受信した前記新たな応答装置識別データで書き換える第2の更新手段とを備えるようにしてもよい。

【0013】また、好ましい態様として、前記応答装置識別データおよびマスタ・キー・グループ識別データは、例えば請求項9記載のように、外部設定装置により無線通信により書換可能であってもよい。

【0014】

【発明の実施の形態】以下、本発明の実施の形態を、自動販売機に適用した一実施例として、図面を参照して説明する。

#### A. 実施例の構成

##### A-1. 自動販売機に内蔵されるリーダおよび鍵（トランスポンダ）の構成

図1は本発明の実施例による自動販売機に内蔵されるリーダおよびトランスポンダが内蔵された、自動販売機の錠を開錠するための鍵の構成を示すブロック図である。また、図4は、上記トランスポンダのより詳細な構成例を示すブロック図である。図において、リーダ1は、自動販売機に内蔵されており、変調回路2、RFパワー送信機3、DATA受信回路4、DATA復調回路5、MPU6、NG表示用LED13、リレー14、スイッチングレギュレータ15等から構成されている。以下、各部について説明する。

【0015】変調回路2は、所定の信号を125KHzでFSK変調し、RFパワー送信機3に供給する。RFパワー送信機3は、上記変調信号をアンテナ16より送信する。上記信号としては、鍵に内蔵されている後述するトランスポンダ18を作動させるためのRFパワーや、トランスポンダ18に対して各種ID送信を要求するためのコマンドがある。次に、DATA受信回路4は、後述するトランスポンダ18から送信される、62.5KHzでPSK変調された信号をアンテナ17で受信し、DATA復調回路5に供給する。DATA復調回路5は、受信信号を復調し、データ（各種ID）を取り出し、MPU6のSIO（シリアル入出力インターフェース）7へ供給する。

【0016】MPU6は、上記SIO7、CPU（中央処理装置）8、EEPROM9、ROM（リードオンリ

メモリ10、RAM(ランダムアクセスメモリ)11およびPIO(パラレル入出力インターフェース)12から構成されている。SIO7は、上記DATA復調回路5からのデータをCPU8に供給する。CPU8は、ROM10に格納されているプログラムを実行し、各種コマンドの送信、トランスポンダ18からの各種データの受信、トランスポンダ18の認証、後述するリレー駆動による電気錠20の開錠等の制御を行う。EEPROM9には、自動販売機に内蔵された当該リーダ1に対応するトランスポンダ18を識別するための各種IDデータが記憶されている。言い換えると、本リーダ1は、該EEPROM9に記憶されているIDデータに一致するIDデータを送信するトランスポンダ18が近接した場合にのみ、電気錠20を開錠するようになっている。

【0017】また、ROM10には、上述したように、CPU8によって実行されるプログラムが格納されている。RAM11は、上記CPU8の制御に伴って生成されるデータが格納されたり、ワーキングエリアとして用いられる。PIO12は、CPU8の制御の下、CPU8から供給される表示データをNG表示用LED13に供給するとともに、CPU8から供給されるリレー駆動用データをリレー14に供給する。NG表示用LED13は、トランスポンダ18から送信されるIDデータが上記EEPROM9に格納されているIDデータと不一致である場合、すなわち、適合しないトランスポンダで開錠されようとした場合に、点灯される表示部である。次に、リレー14は、上記リレー駆動用データが供給されると、電気錠20を作動させて開錠する。スイッチングレギュレータ15は、図示しない商用電源を整流し、直流電圧として、+5V、+24Vを発生し、上述した各部へ電源として供給する。

【0018】また、鍵穴21は、例えば、自動販売機の前面に設けられている。但し、本実施例では、以下において、鍵穴21を設ける場合と、鍵穴21を設けない場合とについて説明している。また、鍵穴21は、いわゆるダミーであり、操作しやすい場所であれば、特に、電気錠20が配設されている場所を避ければ、どこに設けてもよい。これは、仮に、鍵穴21が破壊されても、電気錠自体を破壊することができないようにするためである。検出回路25は、上記鍵穴21に鍵が挿入されたことを検出し、PIO12を介してCPU8に知らせる。このように、鍵穴21を設けた場合には、CPU8は、RFパワー送信機3からRFパワー信号を送信する。

#### 【0019】A-2. 自動販売機の外観構成

図2および図3は、上述したリーダが内蔵された自動販売機の外観構成を示す斜視図である。本実施例では、トランスポンダを内蔵する鍵として、カード形状のものと、通常の鍵形状のものの2つの構成例を採用している。したがって、トランスポンダ18にカード形状のものを採用した場合には、図2に示すように、自動販売機

には、鍵穴はなく、トランスポンダ18からのID認証によって開錠される電気錠のみが設けられている。また、トランスポンダ18に通常の鍵形状のものを採用した場合には、図3に示すように、自動販売機には、上記トランスポンダ18からのID認証によって開錠される電気錠とともに、該鍵が差し込まれる鍵穴21が設けられている。この場合、鍵穴21は、上述したように、鍵を挿入することで、実際に機械式の錠を開けるためのものではなく、トランスポンダ18が内蔵された鍵が挿入されたことを検知することで、メンテナンス等のために、開錠しようとしていることを認識するために用いられるものである。

【0020】本実施例では、鍵に内蔵されているトランスポンダ18は、自動販売機に内蔵されたリーダ1から送信されるRFパワー信号を電源として作動するようになっている。したがって、鍵にカード形状のものを採用した場合には、いつ鍵がリーダ1の通信範囲に入ったかを知ることができないため、常時あるいは所定時間間隔で、RFパワー信号を送信しなければならない。これに対して、自動販売機に鍵穴を設けた場合には、リーダ1は、鍵が自動販売機の鍵穴に挿入された時点で、RFパワー信号を送信し、トランスポンダ18を作動させればよく、省電力化に効果がある。また、上記鍵穴が実際に開閉するための電気錠のものではないので、鍵穴は、必ずしも電気錠部分に設ける必要はない。したがって、鍵穴をこじ開けることにより、不正に開錠しようとしても、開錠することはできず、また、仮に鍵穴が破壊されたとしても、鍵穴修理に要する金額が小さいので、容易に修理できる。

#### 【0021】A-3. トランスポンダの構成

図4(a)、(b)は、上述したトランスポンダ18の構成例を示すブロック図である。図4(a)に示すトランスポンダ18は、アンテナ19、送受信回路22、CPU23、EEPROM24から構成されている。アンテナ19は、上述したリーダ1から送信されるRFパワー信号や変調信号を受信し、送受信回路22に供給する。送受信回路22は、図示しない整流回路を備えており、受信したRFパワー信号を整流して所定の直流電圧を取り出し、CPU23およびEEPROM24に電源として供給するとともに、受信信号を復調し、リーダ1から送信される各種コマンドを取り出してCPU23に供給する。

【0022】CPU23は、プログラムを内蔵するROMやワークエリアとしてのRAM等を内蔵しており(図示略)、RFパワー信号により作動し、リーダ1から送信される各種コマンドを解釈し、受信したコマンドに応じて、EEPROM24に予め格納されている各種IDデータを読み出し、送受信回路22によって変調してアンテナ19から送信する。EEPROM24には、上述したように、予め各種IDデータが記憶されており、該

各種IDデータは、CPU23によって適宜読み出される。このように、図4(a)に示すトランスポンダ18を採用した場合には、トランスポンダ18は、リーダ1からのIDデータ要求コマンドに応じて、対応するIDデータを送信する。

【0023】ここで、図5は、上記リーダ1と上記トランスポンダ18とで授受されるデータフォーマットを示す概念図である。図示するように、データは、スタートビット、データ(12ビット)、パリティビット、ストップビットから構成されており、1キャラクタ単位で、データ部分で各種IDデータを送信し、その後エラーチェック用のデータを同一フォーマットで1キャラクタ送信する。この場合、トランスポンダ18は、図6に示すように、リーダ1からの要求に応じて、システム識別IDデータ、マスターキーグループIDデータおよび鍵IDデータを送信するようになっている。すなわち、トランスポンダ18は、リーダ1からRFパワーを受信すると、まず、自動的に、システム識別IDデータを送信し、次いで、マスターキーグループID要求コマンドを受信すると、これに応じて、マスターキーグループIDデータを送信し、さらに、鍵ID要求コマンドを受信すると、これに応じて、鍵IDデータを送信する。

【0024】なお、システム識別IDデータは、例えば、自動販売機のメーカ毎に設定され、該メーカを識別するためのIDデータであり、固定値となっている。また、マスター・キー・グループIDデータは、自動販売機の設置場所でグループ化し、該グループを識別するためのIDデータであり、変更可能となっている。さらに、鍵IDデータは、トランスポンダ(鍵)18を識別するためのIDデータであり、やはり変更可能となっている。リーダ1は、これらシステム識別IDデータ、マスターキーグループIDデータおよび鍵IDデータの全てが一致した場合にのみ、電気錠を開錠するようになっている。

【0025】一方、図4(b)に示すトランスポンダ18は、アンテナ19、送受信回路26およびEEPROM27から構成されている。アンテナ19は、上述したリーダ1から送信されるRFパワー信号や変調信号を受信し、送受信回路26に供給する。送受信回路26は、図示しない整流回路を備えており、受信したRFパワー信号を整流して所定の直流電圧を取り出し、EEPROM27に電源として供給するとともに、EEPROM27から供給される各種IDデータを変調し、アンテナ19から送信する。EEPROM27には、上述したように、予め各種IDデータが記憶されており、電源が供給されると、記憶されていた各種IDデータを自動的に送受信回路26に供給する。このように、図4(b)に示すトランスポンダ18を採用した場合には、トランスポンダ18は、RFパワー信号を受信した時点で、EEPROM27に予め記憶されている各種IDデータを送信

する。

【0026】ここで、図7は、上記リーダと上記トランスポンダとで授受されるデータフォーマットを示す概念図である。図示するように、データは、スタートビット(8ビット)、システム識別IDデータ(16ビット)、マスターキーグループIDデータ(24ビット)、鍵IDデータ(24ビット)、データBCC(16ビット)、ストップビット(8ビット)の全128ビットから構成されている。この場合、トランスポンダ18は、図8に示すように、RFパワーを受信することで作動すると、自動的に、上記データフォーマットで、システム識別IDデータ、マスターキーグループIDデータおよび鍵IDデータを送信するようになっている。なお、システム識別IDデータ、マスターキーグループIDデータおよび鍵IDデータの目的およびその内容は、前述した通りである。

【0027】B. 実施例の動作

次に、上述した実施例による自動販売機に内蔵されたリーダ1および鍵に内蔵されたトランスポンダ18の動作について説明する。なお、以下では、上述したリーダ、トランスポンダ、データフォーマットの組み合わせに応じて、以下のケースについて各々の動作を説明する。

①CPU有り、ID更新機能有り

②CPU有り、ID更新機能無し

③CPU無し、ID更新機能有り

④CPU無し、ID更新機能無し

また、以下では、CPU有り、ID更新機能有り・無し、およびCPU無し、ID更新機能有り・無しにおけるIDデータ設定処理の動作についても説明する。

【0028】B-1. 開錠処理(①CPU有り、ID更新機能有り)

まず、CPU23を備えるトランスポンダ(ID更新機能有り)18を用いた場合における開錠処理について説明する。ここで、図9および図10は、CPU23を備えるトランスポンダ(ID更新機能有り)18における、リーダ1およびトランスポンダ18での開錠処理の動作を説明するためのフローチャートである。

【0029】まず、自動販売機のリーダ1では、図9に示すステップS10で、鍵穴に鍵が挿入されたか否かを判断し、鍵が挿入されると、ステップS12で、RFパワー信号を送信する。なお、カード状の鍵を用いた場合には、後述するステップS14でデータを受信するまで、所定時間間隔で、RFパワー信号の送信を繰り返す。

【0030】これに対して、鍵のトランスポンダ18は、上記RFパワー信号を受信することで作動し、図10に示すステップS40で、EEPROM24からシステム識別IDデータ、マスター・キー・グループIDデータおよび鍵IDデータを読み込む。次に、ステップS42で、図5に示すデータフォーマットで、システム識別

IDデータを送信する。

【0031】リーダ1では、ステップS14で、上記システム識別IDデータを受信し、ステップS16で、自身のEEPROM9に予め設定されているシステム識別IDデータと照合し、一致すれば、ステップS18に進み、マスタ・キー・グループIDデータ要求コマンドを送信する。これに対して、鍵のトランスポンダ18では、ステップS44で、上記マスタ・キー・グループIDデータ要求コマンドを受信すると、ステップS46で、ステップS40で読み出したマスタ・キー・グループIDデータを図5に示すデータフォーマットで送信する。リーダ1では、ステップS20で、上記マスタ・キー・グループIDデータを受信する。自動販売機のリーダ1では、上記ステップS18、S20、鍵のトランスポンダ18では、上記ステップS44、S46を繰り返すことにより、鍵IDデータ要求コマンドの送受信、および鍵IDデータの送受信を行い、図5に示すデータフォーマットで鍵IDデータを授受する。

【0032】次に、自動販売機のリーダ1では、ステップS22で、上記マスタ・キー・グループIDデータおよび鍵IDデータを、EEPROM9に予め設定されているIDデータと照合することにより、一致するか否かを判断し、それぞれ一致すると、ステップS24に進み、リレー14を駆動し、電気錠20を開く。そして、ステップS26で、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を乱数によって生成し、EEPROM9のIDデータを更新し、記憶する。次に、ステップS28で、上記新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を送信する。

【0033】これに対して、鍵のトランスポンダ18では、ステップS48で、上記新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を受信し、該新たなIDデータで、EEPROM24のIDデータを書き換え、更新する。

【0034】さらに、自動販売機のリーダ1では、ステップS30で、システム運用データとして、開錠した日時、開錠に用いられたトランスポンダ（鍵またはカード）18を識別するための鍵IDデータ（個別かマスタか）を記録する。

【0035】また、リーダ1において、ステップS16で、トランスポンダ18から送信されたシステム識別IDが自身のものと一致しない場合、あるいは、ステップS22で、トランスポンダ18から送信されたマスタ・キー・グループIDデータあるいは鍵IDデータが自身のものと一致しない場合には、ステップS32で、防犯および警報システムを作動させる。

【0036】B-2. 開錠処理（②CPU有り、ID更新機能無し）

次に、CPU23を備えるトランスポンダ（ID更新機

能無し）18を用いた場合における開錠処理について説明する。ここで、図11および図12は、CPU23を備えるトランスポンダ（ID更新機能無し）18における、リーダ1およびトランスポンダ18での開錠処理の動作を説明するためのフローチャートである。

【0037】まず、リーダ1では、図11に示すステップS60で、鍵穴に鍵が挿入されたか否かを判断し、鍵が挿入されると、ステップS62で、RFパワー信号を送信する。なお、カード状の鍵を用いた場合には、後述するステップS64でデータを受信するまで、所定時間間隔で、RFパワー信号の送信を繰り返す。

【0038】これに対して、鍵のトランスポンダ18は、上記RFパワー信号を受信することで作動し、図12に示すステップS80で、EEPROM24からシステム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータを読み込む。次に、ステップS82で、図5に示すデータフォーマットで、システム識別IDデータを送信する。

【0039】リーダ1では、ステップS64で、上記システム識別IDデータを受信し、ステップS66で、自身のEEPROM9に予め設定されているシステム識別IDデータと照合し、一致すれば、ステップS68に進み、マスタ・キー・グループIDデータ要求コマンドを送信する。

【0040】これに対して、鍵のトランスポンダ18では、ステップS84で、上記マスタ・キー・グループIDデータ要求コマンドを受信すると、ステップS86で、ステップS80で読み出したマスタ・キー・グループIDデータを図5に示すデータフォーマットで送信する。リーダ1では、ステップS70で、上記マスタ・キー・グループIDデータを受信する。そして、自動販売機のリーダ1では、上記ステップS68、S70、鍵のトランスポンダ18では、上記ステップS84、S86を繰り返すことにより、鍵IDデータ要求コマンドの送受信、および鍵IDデータの送受信を行い、図5に示すデータフォーマットで鍵IDデータを授受する。

【0041】次に、自動販売機のリーダ1では、ステップS72で、上記マスタ・キー・グループIDデータおよび鍵IDデータを、EEPROM9に予め設定されているデータと照合することにより、一致するか否かを判断し、それぞれ一致すると、ステップS74に進み、リレー14を駆動し、電気錠20を開く。さらに、自動販売機のリーダ1では、ステップS76で、システム運用データとして、開錠した日時、開錠に用いられたトランスポンダ（鍵またはカード）18を識別するための鍵IDデータ（個別かマスタか）を記録する。

【0042】また、リーダ1において、ステップS66で、トランスポンダ18から送信されたシステム識別IDが自身のものと一致しない場合、あるいは、ステップS72で、トランスポンダ18から送信されたマスタ・



キー・グループIDデータあるいは鍵IDデータが自身のものと一致しない場合には、ステップS78で、防犯および警報システムを作動させる。

【0043】B-3. 開錠処理(③CPU無し、ID更新機能有り)

次に、CPUを備えていないトランスポンダ(ID更新機能有り)18を用いた場合における開錠処理について説明する。ここで、図13および図14は、CPUを備えていないトランスポンダ(ID更新機能有り)18における、リーダ1およびトランスポンダ18での開錠処理の動作を説明するためのフローチャートである。

【0044】まず、自動販売機のリーダ1では、図13に示すステップS90で、鍵穴に鍵が挿入されたか否かを判断し、鍵が挿入されると、ステップS92で、RFパワー信号を送信する。なお、カード状の鍵を用いた場合には、後述するステップS94でデータを受信するまで、所定時間間隔で、RFパワー信号の送信を繰り返す。

【0045】これに対して、鍵のトランスポンダ18は、上記RFパワー信号を受信することで作動し、図14に示すステップS110で、EEPROM27からシステム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータを読み込む。次に、ステップS112で、図7に示すデータフォーマットで、システム識別IDデータマスタ・キー・グループIDデータおよび鍵IDデータを送信する。

【0046】リーダ1では、ステップS94で、上記システム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータを受信し、ステップS96で、自身のEEPROM9に予め設定されているシステム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータと照合し、一致すれば、ステップS98に進み、リレー14を駆動し、電気錠20を開く。そして、ステップS100で、新たなIDデータ(マスタ・キー・グループIDデータまたは/および鍵IDデータ)を乱数によって生成し、EEPROM9のIDデータを更新し、記憶する。次に、ステップS102で、上記新たなIDデータ(マスタ・キー・グループIDデータまたは/および鍵IDデータ)を送信する。

【0047】これに対して、鍵のトランスポンダ18では、ステップS114で、上記新たなIDデータ(マスタ・キー・グループIDデータまたは/および鍵IDデータ)を受信し、ステップS116で、該新たなIDデータで、EEPROM27のIDデータを書き換え、更新する。

【0048】さらに、自動販売機のリーダ1では、ステップS104で、システム運用データとして、開錠した日時、開錠に用いられたトランスポンダ(鍵)18を識別するための鍵IDデータ(個別かマスタか)を記録する。

【0049】また、リーダ1において、ステップS96で、トランスポンダ18から送信されたシステム識別ID、マスタ・キー・グループIDデータまたは鍵IDデータのいずれか1つでも自身のものと一致しない場合には、ステップS106で、防犯および警報システムを作動させる。

【0050】B-4. 開錠処理(④CPU無し、ID更新機能無し)

次に、CPUを備えていないトランスポンダ(ID更新機能無し)18を用いた場合における開錠処理について説明する。ここで、図15および図16は、CPUを備えていないトランスポンダ(ID更新機能無し)18における、リーダ1およびトランスポンダ18での開錠処理の動作を説明するためのフローチャートである。

【0051】まず、自動販売機のリーダ1では、図15に示すステップS120で、鍵穴に鍵が挿入されたか否かを判断し、鍵が挿入されると、ステップS122で、RFパワー信号を送信する。なお、カード状の鍵を用いた場合には、後述するステップS124でデータを受信するまで、所定時間間隔で、RFパワー信号の送信を繰り返す。

【0052】これに対して、鍵のトランスポンダ18は、上記RFパワー信号を受信することで作動し、図16に示すステップS140で、EEPROM27からシステム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータを読み込む。次に、ステップS142で、図7に示すデータフォーマットで、システム識別IDデータマスタ・キー・グループIDデータおよび鍵IDデータを送信する。

【0053】リーダ1では、ステップS124で、上記システム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータを受信し、ステップS126で、自身のEEPROM9に予め設定されているシステム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータと照合し、一致すれば、ステップS128に進み、リレー14を駆動し、電気錠20を開く。さらに、自動販売機のリーダ1では、ステップS130で、システム運用データとして、開錠した日時、開錠に用いられたトランスポンダ(鍵またはカード)18を識別するための鍵IDデータ(個別かマスタか)を記録する。

【0054】また、リーダ1において、ステップS126で、トランスポンダ18から送信されたシステム識別ID、マスタ・キー・グループIDデータまたは鍵IDデータのいずれか1つでも自身のものと一致しない場合には、ステップS132で、防犯および警報システムを作動させる。

【0055】B-5. IDデータ設定処理(CPU有り)

次に、CPU23を備えるトランスポンダ18を用いた



場合におけるIDデータ設定処理について説明する。当該IDデータ設定処理は、自動販売機の出荷時、鍵の紛失、盗難あるいは鍵穴の破壊などの場合に、リーダ1およびトランスポンダ18に既に設定されているIDデータ（マスターキーグループIDデータまたは／および鍵IDデータ）を変更する場合に実行される。ここで、図17ないし図19は、CPU23を備えるトランスポンダ（ID更新機能有り・無し）18における、設定器（図示略）、リーダ1およびトランスポンダ18におけるIDデータ設定処理の動作を説明するためのフローチャートである。

【0056】図示しない設定器では、まず、ステップS150で、新IDデータ（マスターキーグループIDデータまたは／および鍵IDデータ）が設定され、リーダ1のデータ通信範囲内に移動させられる。そして、リーダ1のデータ通信範囲内に移動すると、ステップS152で、自動販売機のリーダ1に対してシステム識別IDデータを送信する。

【0057】これに対して、自動販売機のリーダ1では、設定器が該リーダの通信範囲内に移動した時点で、図18に示すステップS160において、設定器から送信されるデータ（システム識別ID）を自動的に受信する。次に、データを受信すると、ステップS162で、受信したデータがEEPROM9に予め設定されているシステム識別IDと一致するか照合し、一致すると、ステップS164に進み、設定器に対してマスタ・キー・グループIDデータ要求コマンドを送信する。

【0058】設定器では、ステップS154で、リーダ1からマスタ・キー・グループIDデータ要求コマンドを受信すると、ステップS156で、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を設定するというコマンド、言い換えると、マスタ・キー・グループIDデータ要求コマンドに対するマスタ・キー・グループIDデータ以外の所定のデータを、自動販売機のリーダ1に対して送信した後、ステップS158で、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）をリーダ1に対して送信する。

【0059】自動販売機のリーダ1では、ステップS166で、マスタ・キー・グループIDデータ要求に対するデータを受信し、ステップS168で、受信したデータが新たなIDデータの設定データ（コマンド）であるか判断し、設定データであると、ステップS170に進み、設定器から送信された新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を受信する。次に、ステップS172で、受信した新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）でEEPROM9に格納されているIDデータを更新し、記憶する。そして、ステップS174で、鍵のトランスポンダ18に対して、

上記新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を送信する。

【0060】これに対して、鍵のトランスポンダ18では、当該トランスポンダ18がリーダのデータ通信範囲にあると、図19に示すステップS190で、新IDデータを自動的に受信し、ステップS192で、受信した新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）でEEPROM24に格納されているIDデータを更新し、記憶する。

【0061】一方、リーダ1では、図18に示すステップS176で、システムのIDデータ変更完了処理として、鍵のトランスポンダ18との間でIDデータを授受することにより、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）の変更を確認する。そして、ステップS178で、システム運用データとして、IDデータを変更（設定）した日時、トランスポンダ（鍵）18を識別するための鍵IDデータ（個別かマスタか）、およびIDデータを変更（設定）したことを記録する。

【0062】また、自動販売機のリーダ1において、ステップS162で、設定器から送信されたシステム識別IDと自身のシステム識別IDとが一致しない場合、あるいは、ステップS168で、受信したデータが新たなIDデータの設定データ（コマンド）でない場合には、ステップS180で、防犯および警報システムを作動させる。

【0063】このように、上述した処理によれば、CPU23を備えているトランスポンダ18を用いる場合には、新たなIDデータを設定する際に、システムIDデータを自動販売機のリーダ1に送信するとともに、リーダ1からのマスタ・キー・グループIDデータ要求コマンドに対して所定のデータを送信することで、該リーダ1を自動的に新たなIDデータ受信処理へ移行させることができる。したがって、リーダ1およびトランスポンダ18は、通常のデータ授受処理と同様のデータ授受処理を行うことで、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を設定することができる。

【0064】B-6. IDデータ設定処理（CPU無し）

次に、CPUを備えていないトランスポンダ18を用いた場合におけるIDデータ設定処理について説明する。ここで、図20ないし図21は、CPUを備えていないトランスポンダ（ID更新機能有り・無し）18における、設定器（図示略）、リーダ1およびトランスポンダ18におけるIDデータ設定処理の動作を説明するためのフローチャートである。

【0065】図示しない設定器では、まず、図20に示すステップS200で、新IDデータ（マスターキーグループIDデータまたは／および鍵IDデータ）が設定

され、リーダ1のデータ通信範囲内に移動させられる。そして、リーダ1のデータ通信範囲内に移動すると、ステップS202で、自動販売機のリーダ1に対して、設定器を識別するための設定器IDデータを送信した後、ステップS204で、新たなIDデータを送信する。

【0066】これに対して、自動販売機のリーダ1では、設定器が通信範囲内に移動した時点で、図21に示すステップS210において、設定器から送信される設定器IDデータを受信的に受信する。次に、設定器IDデータを受信すると、ステップS212で、受信した設定器IDデータが所定のデータであるか照合し、所定のデータである場合には、ステップS214に進み、設定器から送信される新たなIDデータを受信する。

【0067】次に、リーダ1は、ステップS216で、受信した新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）でEEPROM9に格納されているIDデータを更新し、記憶する。そして、ステップS218で、鍵のトランスポンダ18に対して、上記新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を送信する。

【0068】これに対して、鍵のトランスポンダ18では、当該トランスポンダ18がリーダ1のデータ通信範囲にあると、図22に示すステップS230で、新IDデータを自動的に受信し、ステップS232で、受信した新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）でEEPROM27に格納されているIDデータを更新し、記憶する。

【0069】一方、リーダ1では、図21に示すステップS220で、システムのIDデータ変更完了処理として、鍵のトランスポンダ18との間でIDデータを授受することにより、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）の変更を確認する。そして、ステップS222で、システム運用データとして、IDデータを変更（設定）した日時、トランスポンダ（鍵）18を識別するための鍵IDデータ（個別かマスタか）およびIDデータを変更（設定）したことを記録する。

【0070】また、自動販売機のリーダ1において、ステップS212で、設定器から送信された設定器IDデータが所定のデータでない場合には、ステップS224で、防犯および警報システムを作動させる。

【0071】このように、上述した処理によれば、CPU23を備えていないトランスポンダ18を用いる場合、新たなIDデータを設定する際に、設定器固有の設定器IDデータを自動販売機のリーダ1に送信することで、該リーダ1を自動的に新たなIDデータ受信処理へ移行させることができる。したがって、リーダ1およびトランスポンダ18は、通常のデータ授受処理と同様のデータ授受処理を行うことで、新たなIDデータ（マ

スタ・キー・グループIDデータまたは／および鍵IDデータ）を設定することができる。

【0072】なお、上記実施例では、鍵のトランスポンダと自動販売機のリーダとのIDデータが不一致である場合、防犯および警報システムを作動させるようにしたが、具体的には、警報音を鳴らしたり、防犯カメラを作動させたり、通信回線を介して通報したりというように、少なくとも1つ、あるいはこれらを組み合わせて用いる。

10 【0073】

【発明の効果】請求項1記載の発明によれば、応答装置が自動販売機に近接すると、読み取り装置の高周波発生手段からの高周波磁界を電力とし、第1の送信手段から第1の記憶手段に記憶されている応答装置識別データが送信され、該応答装置識別データが読み取り装置の第2の記憶手段に記憶されている応答装置識別データとが一致すると、電気錠が開錠されるようにしたので、外部から錠の位置が分からず、錠の破壊を防止することができるという利点が得られる。

20 【0074】また、請求項2記載の発明によれば、前記第1受信手段によって受信された応答装置識別データと前記第2の記憶手段に記憶されている応答装置識別データとが一致しない場合、警告手段によって警告を発するようにしたので、不正な応答装置または不正な鍵による開錠、もしくは錠の破壊を防止することができるという利点が得られる。

【0075】また、請求項3記載の発明によれば、前記応答装置を鍵形状部分とし、前記自動販売機の前記電気錠が設けられる位置とは異なる位置に、前記応答装置の鍵形状部分が挿入される鍵穴部を備え、前記読み取り装置は、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことを検知する検出手段を備えるようにしたので、仮に錠穴が破壊されても、電気錠でロックされますので、扉を開けることはできず、盗難を防止することができる、かつ、電気錠自体が破壊されることは避けられるので、被害規模を最小にすることができるという利点が得られる。

【0076】また、請求項4記載の発明によれば、前記読み取り装置の前記検出手段によって、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことが検知された時点で、前記高周波発生手段によって高周波磁界を発生するようにしたので、電力消費を低減することができるという利点が得られる。

【0077】また、請求項5記載の発明によれば、前記応答装置をカード形状とし、前記読み取り装置の前記高周波発生手段によって所定時間間隔で前記高周波磁界を発生するようにしたので、自動販売機に鍵穴を設ける必要がなく、錠の破壊を防止することができるという利点が得られる。

50 【0078】また、請求項6記載の発明によれば、前記

応答装置および前記読み取り装置は、前記応答装置識別データに加えて、システムを識別するシステム識別データおよび自動販売機の設置地域を識別するマスタ・キー・グループ識別データを授受するようにしたので、より安全性を向上させることができるという利点が得られる。

【0079】また、請求項7記載の発明によれば、前記応答装置に、所定の通信プロトコルに従って、前記読み取り装置との間におけるデータ授受を制御する第2の制御手段を備え、前記応答装置および前記読み取り装置との間で、前記所定の通信プロトコルに従って、前記システム識別データ、前記マスタ・キー・グループ識別データおよび前記応答装置識別データを授受するようにしたので、より機密性を向上させることができ、より安全性を向上させることができるという利点が得られる。

【0080】また、請求項8記載の発明によれば、電気錠を開錠する度に、認証に必要な応答装置識別データを書き換えるようにしたので、より機密性を向上させることができ、より安全性を向上させることができるとともに、応答装置の不正なコピーを防止できるという利点が得られる。

【0081】また、請求項9記載の発明によれば、前記応答装置識別データおよびマスタ・キー・グループ識別データを外部設定装置により無線通信により書換可能とするようにしたので、応答装置（鍵）の紛失、盗難あるいは鍵穴の破壊が生じた場合でも、非接触で識別データの書き換えができるので、ハードウェアを取り替えることなく、更新できるという利点が得られる。

【図面の簡単な説明】

【図1】本発明の実施例による自動販売機システムの構成を示すブロック図である。

【図2】トランスポンダがカード形状の場合におけるリーダが内蔵された自動販売機の外觀構成を示す斜視図である。

【図3】トランスポンダが鍵状の場合におけるリーダが内蔵された自動販売機の外觀構成を示す斜視図である。

【図4】トランスポンダのより詳細な構成例を示すブロック図である。

【図5】トランスポンダがCPUを備える場合におけるリーダとトランスポンダとで授受されるデータフォーマットを示す概念図である。

【図6】トランスポンダがCPUを備える場合におけるリーダとトランスポンダとの間でのデータ授受を示す概念図である。

【図7】トランスポンダがCPUを備えない場合におけるリーダとトランスポンダとで授受されるデータフォーマットを示す概念図である。

【図8】トランスポンダがCPUを備えない場合におけるリーダとトランスポンダとの間でのデータ授受を示す概念図である。

【図9】CPUを備えるトランスポンダ（ID更新機能有り）の場合における、リーダでの開錠処理の動作を説明するためのフローチャートである。

【図10】CPUを備えるトランスポンダ（ID更新機能有り）の場合における、トランスポンダでの開錠処理の動作を説明するためのフローチャートである。

【図11】CPUを備えるトランスポンダ（ID更新機能無し）の場合における、リーダでの開錠処理の動作を説明するためのフローチャートである。

【図12】CPUを備えるトランスポンダ（ID更新機能無し）の場合における、トランスポンダでの開錠処理の動作を説明するためのフローチャートである。

【図13】CPUを備えていないトランスポンダ（ID更新機能有り）の場合における、リーダでの開錠処理の動作を説明するためのフローチャートである。

【図14】CPUを備えていないトランスポンダ（ID更新機能有り）の場合における、トランスポンダでの開錠処理の動作を説明するためのフローチャートである。

【図15】CPUを備えていないトランスポンダ（ID更新機能無し）の場合における、リーダでの開錠処理の動作を説明するためのフローチャートである。

【図16】CPUを備えていないトランスポンダ（ID更新機能無し）の場合における、トランスポンダでの開錠処理の動作を説明するためのフローチャートである。

【図17】CPUを備えるトランスポンダ（ID更新機能有り・無し）の場合における、設定器（図示略）でのIDデータ設定処理の動作を説明するためのフローチャートである。

【図18】CPUを備えるトランスポンダ（ID更新機能有り・無し）の場合、リーダでのIDデータ設定処理の動作を説明するためのフローチャートである。

【図19】CPUを備えるトランスポンダ（ID更新機能有り・無し）の場合における、トランスポンダでのIDデータ設定処理の動作を説明するためのフローチャートである。

【図20】CPUを備えていないトランスポンダ（ID更新機能有り・無し）の場合における、設定器（図示略）でのIDデータ設定処理の動作を説明するためのフローチャートである。

【図21】CPUを備えていないトランスポンダ（ID更新機能有り・無し）の場合、リーダでのIDデータ設定処理の動作を説明するためのフローチャートである。

【図22】CPUを備えていないトランスポンダ（ID更新機能有り・無し）の場合における、トランスポンダでのIDデータ設定処理の動作を説明するためのフローチャートである。

【符号の説明】

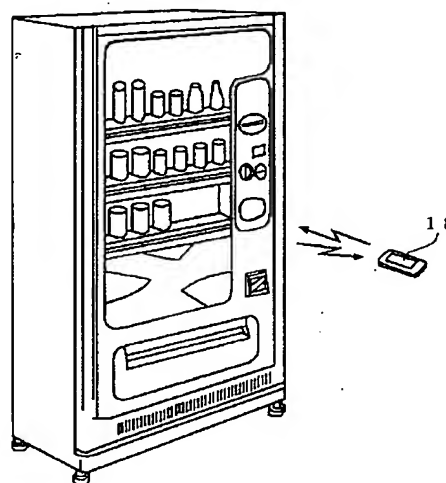
- 1 リーダ
- 2 変調回路（高周波発生手段、第2の送信手段）
- 3 RFパワー送信機（高周波発生手段、第2の送信手

\* 16, 17 アンテナ

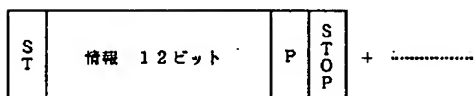
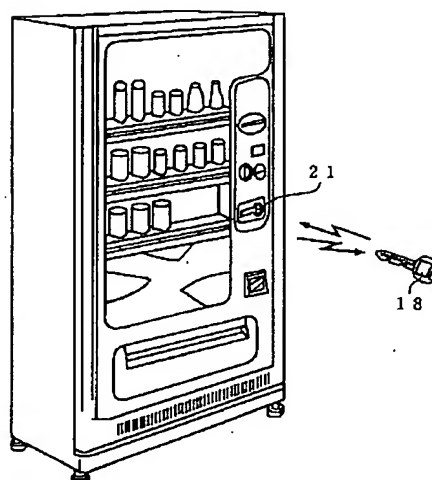
- 18 トランスポンダ
- 19 アンテナ
- 20 電気錠
- 21 鍵穴
- 22 送受信回路（第1の送信手段、第2の受信手段、  
第2の更新手段）
- 23 CPU（第2の制御手段）
- 24 EEPROM（第1の記憶手段）
- 25 検出回路（検出手段）
- 26 送受信回路（第1の送信手段、第2の受信手段、  
第2の更新手段）
- 27 EEPROM（第1の記憶手段）

\*

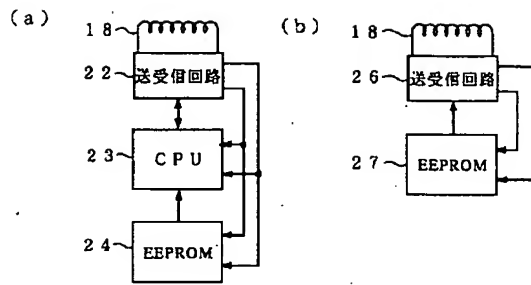
【圖2】



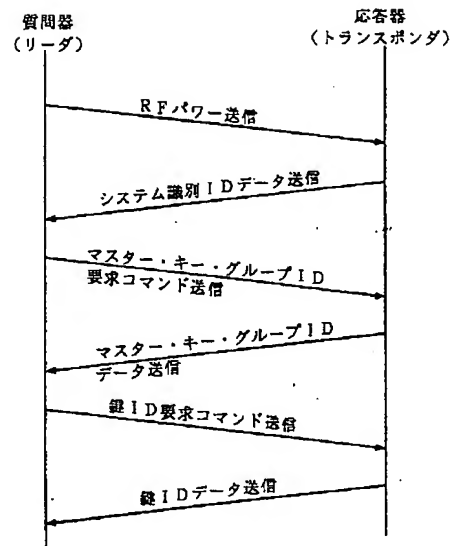
【図5】



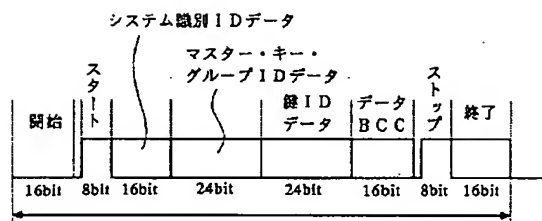
【図4】



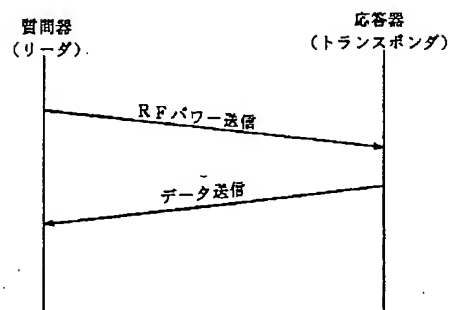
【図6】



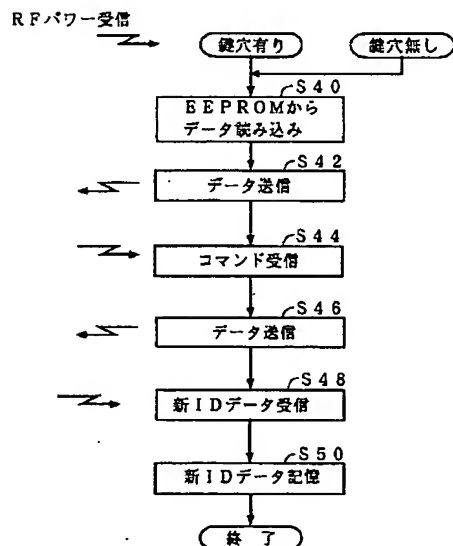
【図7】



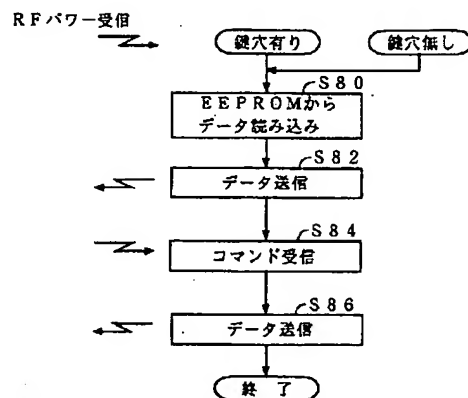
【図8】



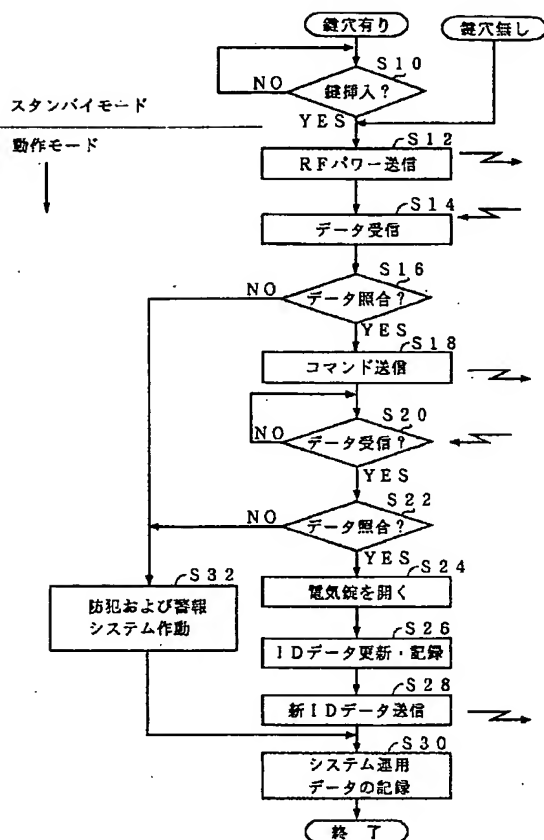
【図10】



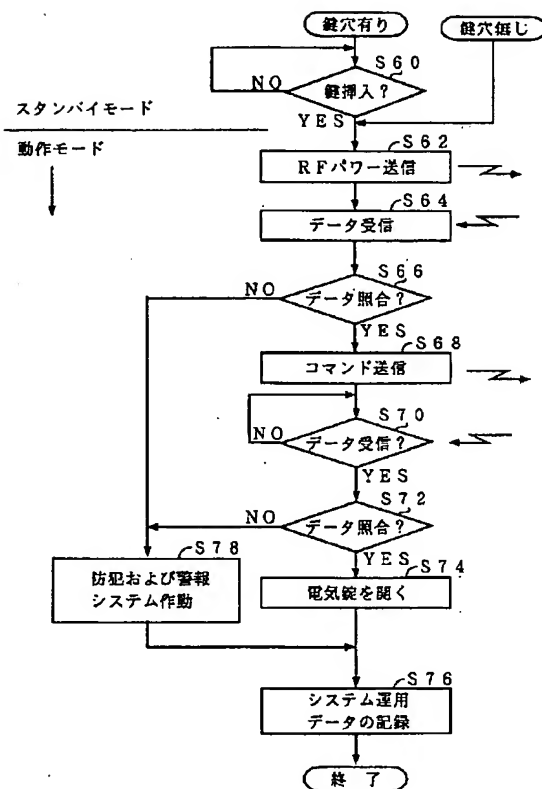
【図12】



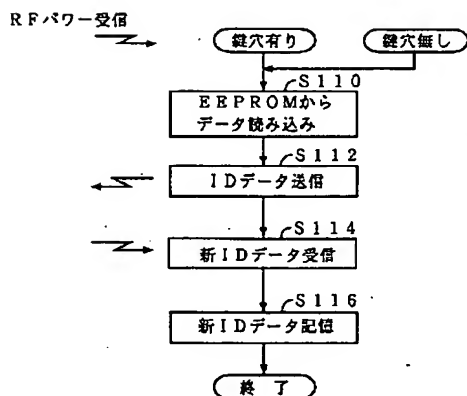
【図9】



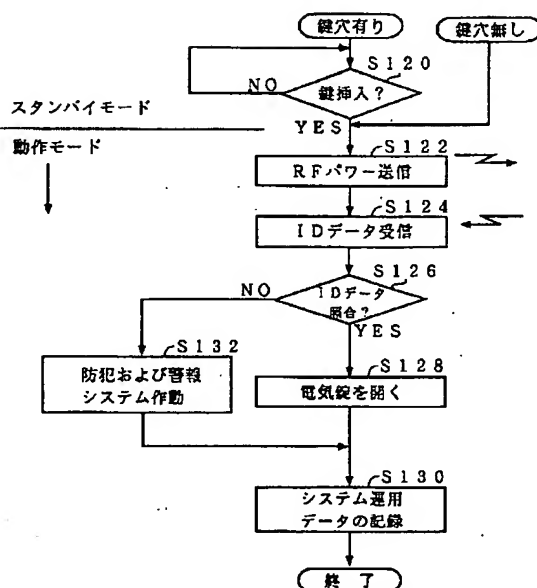
【図11】



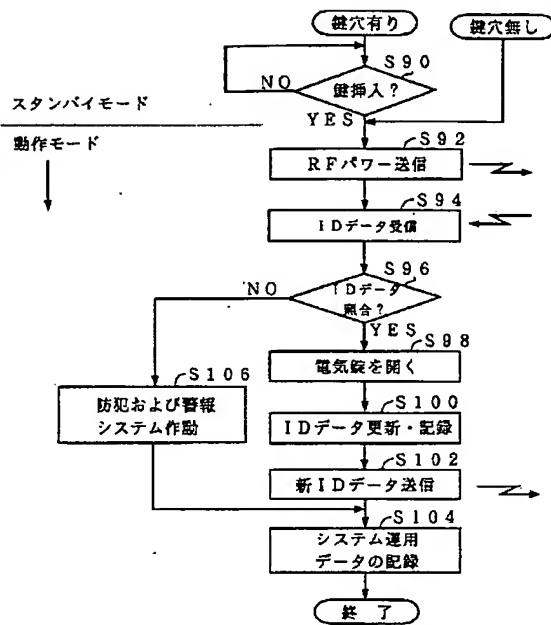
【図14】



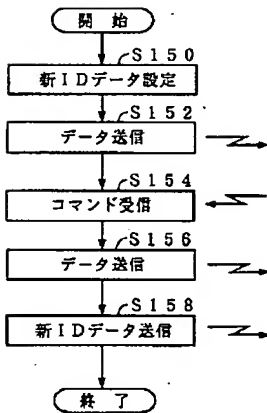
【図15】



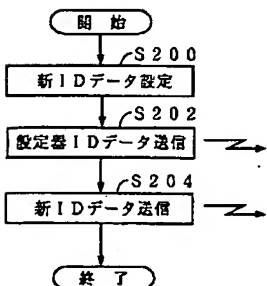
【図13】



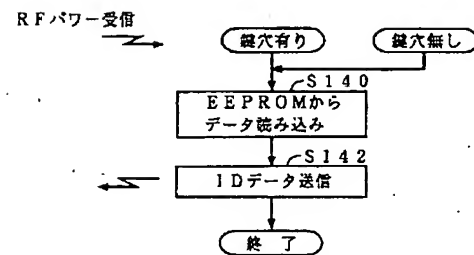
【図17】



【図20】

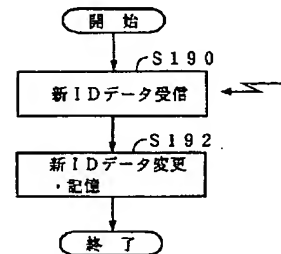


【図16】

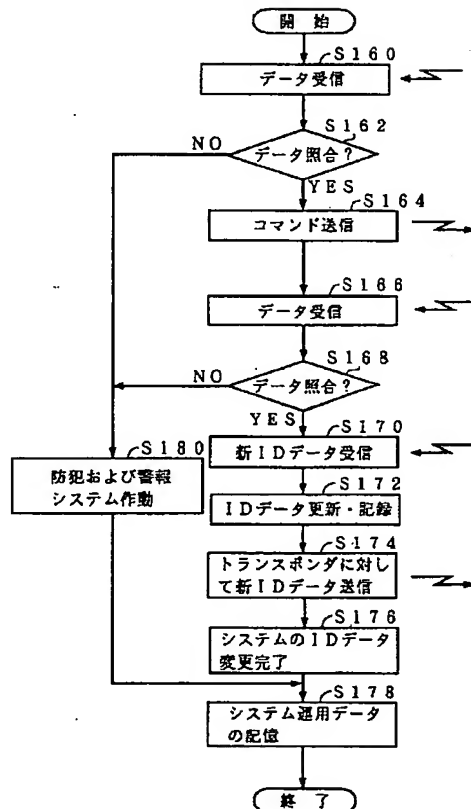


【図19】

IDデータ設定時のトランスポンダ

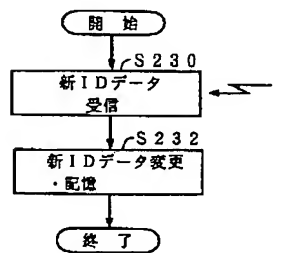


【図18】



【図22】

IDデータ設定時のトランスポンダ





【図21】

